

TITLE OF THE INVENTION

コンテンツ利用管理システム、コンテンツ利用方法及びクライアント機器（CONTENT USE MANAGEMENT SYSTEM, CONTENT USE MANAGEMENT METHOD, AND CLIENT DEVICE）

5

BACKGROUND OF THE INVENTION

(1) Field of the Invention

本発明は、音楽データ及び映像データ等のデジタルコンテンツを配信するサーバとクライアント機器とを備えるコンテンツ利用管理システム、コンテンツ利用方法及びクライアント機器に関する。

10

(2) Description of the Prior Art

ネットワークを介したコンテンツ配信システムにおいて、配信するコンテンツは暗号化され、暗号化コンテンツと暗号化したコンテンツの復号鍵（以下、コンテンツ鍵と略記する）がユーザ端末へ配信される。

15

コンテンツ鍵の配信方式には次の２種類がある。コンテンツの利用を要求してきたクライアント機器にのみ一対一でコンテンツ鍵を配信するユニキャスト配信と、コンテンツの利用を要求していないクライアント機器にも一斉にコンテンツ鍵を配信するマルチキャスト配信である。従来は、１つのコンテンツ配信システムにおいては、コンテンツの種別に関わらずコンテンツ鍵は同一の配信方式にて配信されている。

20

以上のことは文献「特開平 １ １－３ １ ２ １ ７ ５ 号公報」に記載されている。

25

しかしながら、コンテンツ鍵を配信するクライアントの数はコンテンツによって異なる。コンテンツを利用するクライアント機器が多い場合、ユニキャスト配信では各クライアント機器と通信を行った上でコンテンツ鍵を配信するので、ユニキャスト配信よりもマルチキャスト配信を行う方がサーバの負荷が低い。一方、ユニキャスト配信では、どのクライアント機器にどのコンテンツ鍵を配信したかといった情報をログに残すことができるので、著作権を保護する上でマルチキャスト配信よりも高い安全性を確保することができる。従来技術では、コンテンツに関わらずコンテンツ鍵をいずれか一方の配信方式で配信しているので、コンテンツによってはマルチキャスト配信方式でコンテンツ鍵を配信した方がサーバ負荷を軽減できるにもかかわらず

30

らず、サーバ負荷が高い方式で配信されている。また、コンテンツによってはより高い安全性が望まれるにもかかわらず、安全性の低い方式で配信されている。

5 SUMMARY OF THE INVENTION

そこで、本発明では、上記問題点に鑑み、コンテンツに応じて選択的に、システム内の通信負荷を軽減し又はセキュリティを確保してコンテンツ復号鍵を配信できるコンテンツ利用管理システムを提供することを目的とする。

10 本発明におけるコンテンツ利用管理システムは、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、ネットワークを介して配信するコンテンツ利用管理システムであって、前記利用制御データを、クライアント機器へ複数の異なる配信方式により配信する 1 以上の配信サーバと、コンテンツの属性に応じて、各コンテンツの利用制御データを、い
15 ずれの配信方式で配信するかを決定する配信管理サーバとを備え、前記配信サーバのいずれか 1 つは、決定された配信方式による前記利用制御データの配信を実行することを特徴とする。

以上のように、本発明によれば、コンテンツ利用管理システムは複数の異なる配信方式で利用制御データを配信する配信サーバを備え、コンテンツに
20 応じて、利用制御データの配信方式を切り替えることにより、配信サーバの負荷およびセキュリティ確保の観点から最適な配信方式で利用制御データを配信することが可能になる。

また、前記コンテンツの属性は、コンテンツの圧縮フォーマットであって、前記配信管理サーバは、各コンテンツの圧縮フォーマットに応じて、前記利
25 用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツを提供するコンテンツ提供者であって、前記配信管理サーバは、各コンテンツのコンテンツ提供者に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツの圧縮率であって、前記配信
30 管理サーバは、各コンテンツの圧縮率に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記コンテンツの属性は、コンテンツの利用条件であって、前記配

信管理サーバは、各コンテンツの利用条件に応じて、前記利用制御データの配信方式を決定するとしてもよい。

また、前記 1 以上の配信サーバは、クライアント機器からの要求に応じてデータを配信するユニキャスト配信方式により、前記利用制御データを配信
5 するユニキャスト配信手段と、所定の配信時刻に複数のクライアント機器に対して一斉にデータを配信するマルチキャスト配信方式により、前記利用制御データを配信するマルチキャスト配信手段との少なくとも 1 つを備えるとしてもよい。

また、前記配信管理サーバは、前記配信方式を決定するためのルールを示した配信方式決定ルールを保持する配信方式決定ルール保持手段と、前記コ
10 ンテンツの属性に対応する前記配信方式決定ルールを参照し、前記配信方式決定ルールに従って前記配信方式を決定する配信方式決定手段とを備えるとしてもよい。

また、前記ユニキャスト配信手段を備える配信サーバは、さらに、各クライアント機器との通信により、前記クライアント機器があらかじめ登録され
15 たクライアント機器であることを確認できた場合、前記クライアント機器を正当なユーザであると認める認証手段を備え、前記ユニキャスト配信手段は、前記認証手段により、正当なユーザであると認められたクライアント機器に対してのみ前記利用制御データを配信するとしてもよい。

また、前記利用制御データは、暗号化されたコンテンツを復号するための復号鍵を含み、前記クライアント機器は、各コンテンツに対応する利用制御
20 データを、いずれかの前記配信サーバから取得する利用制御データ取得手段と、取得された前記利用制御データから前記復号鍵を抽出し、抽出された復号鍵を用いて前記利用制御データに対応するコンテンツを復号する復号手段と、復号された前記コンテンツを再生する再生手段とを備えるとしてもよい。
25

また、前記利用制御データは、さらに、コンテンツを利用するための条件を示した利用条件を含み、前記クライアント機器は、さらに、取得された前記利用制御データから前記利用条件を抽出し、抽出された利用条件が満足さ
30 れる範囲内で前記再生が行われるよう前記再生手段を制御する再生制御手段を備えるとしてもよい。

さらに、本発明におけるコンテンツ利用管理方法は、クライアント機器に

おけるコンテンツの利用を制御するための利用制御データを、ネットワークを介して配信するサーバのためのコンテンツ利用管理方法であって、コンテンツの属性に応じて、各コンテンツの利用制御データを、いずれの配信方式で配信するかを決定する配信方式決定ステップと、複数の相異なる配信方式のうち、決定された配信方式で前記利用制御データを配信する配信ステップとを含むことを特徴とする。

また、前記コンテンツ利用管理方法では、前記配信方式を決定するためのルールを示した配信方式決定ルールをあらかじめ保持し、前記配信方式決定ステップでは、前記コンテンツの属性に対応する前記配信方式決定ルールを参照し、前記配信方式決定ルールに従って前記配信方式を決定するとしてもよい。

さらに、本発明におけるクライアント機器は、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、コンテンツを配信するコンテンツサーバに対し、コンテンツの配信を要求してコンテンツを取得するコンテンツ要求手段と、前記コンテンツサーバからの前記コンテンツの取得の成否に応じて、要求した前記コンテンツに対応する利用制御データの配信方式を判定する配信方式判定手段と、判定された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えることを特徴とする。以上のように、本発明によれば、マルチキャスト配信される利用制御データがコンテンツに重畳されて配信される場合においても、クライアント機器側で利用制御データの配信方式を判定することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

また、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、コンテンツを配信するコンテンツサーバから、各コンテンツに対応する利用制御データの配信方式を示す情報を含んだコンテンツを取得するコンテンツ取得手段と、取得された前記コンテンツから前記配信方式を示した情報を抽出し、

抽出された前記情報に基づいて、前記コンテンツに対応する利用制御データの配信方式を識別する配信方式識別手段と、識別された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えるとしてもよい。従って、利用制御データの配信方式を示す情報がコンテンツに重畳されている場合においても、クライアント機器側で利用制御データの配信方式を識別することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

また、クライアント機器におけるコンテンツの利用を制御するための利用制御データを、複数の異なる配信方式により、ネットワークを介して配信するコンテンツ利用管理システムにおけるクライアント機器であって、前記利用制御データの配信方式を決定するサーバから、各利用制御データの配信方式を示す情報を取得する方式情報取得手段と、前記配信方式を示す情報に基づいて、前記コンテンツに対応する利用制御データの配信方式を識別する配信方式識別手段と、識別された配信方式で前記利用制御データを配信する配信サーバから、前記利用制御データを取得する利用制御データ取得手段とを備えるとしてもよい。以上のように、利用制御データの配信方式を決定するサーバから、各利用制御データの配信方式を示す情報を取得する場合においても、クライアント機器側で利用制御データの配信方式を識別することができる。これにより、コンテンツに応じて利用制御データの配信方式が異なる場合であっても、問題なく利用制御データを取得し、コンテンツを利用することができる。

なお、本発明は、このようなコンテンツ利用管理システムとして実現することができるだけでなく、これらのコンテンツ利用管理システムを構成するコンテンツ配信管理サーバ、ユーザ管理サーバ、暗号化コンテンツ配信サーバ、ユニキャスト配信サーバ、マルチキャスト配信サーバ及びクライアント機器などの単体として実現したり、これらのコンテンツ利用管理システムにおける特徴的な動作をステップとするコンテンツ利用管理方法として実現したり、その特徴的な動作をパーソナルコンピュータ等の汎用のコンピュータに実行させて機能させるプログラムとして実現することもできる。そして、そのプログラムは、ＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体やインターネット等の伝送媒体を介して頒布することができるのは言うま

でもない。

BRIEF DESCRIPTION OF THE DRAWINGS

図 1 は、本発明におけるコンテンツ配信サービスシステムの概念図である。

5 図 2 は、ユーザ管理 DB の管理データの一例を示す図である。

図 3 は、コンテンツホルダ管理 DB の管理データの一例を示す図である。

図 4 は、コンテンツ配信方式管理 DB の管理データの一例を示す図である。

図 5 (a) は、配信スケジュール DB で保持される配信スケジュール表の更新前の一例を示す図である。

10 図 5 (b) は、配信スケジュール DB で保持される配信スケジュール表の更新後の一例を示す図である。

図 6 は、配信データ管理 DB の管理データの一例を示す図である。

図 7 は、暗号化コンテンツ管理 DB の管理データの一例を示す図である。

15 図 8 (a) は、図 1 に示したユニキャストコンテンツ DB に格納される暗号化コンテンツのデータ構造を示す図である。

図 8 (b) は、図 1 に示したマルチキャストコンテンツ DB に格納される暗号化コンテンツのデータ構造を示す図である。

図 9 は、コンテンツホルダによるコンテンツの登録のフローチャートである。

20 図 10 は、コンテンツのメタデータの一例を示す図である。

図 11 は、コンテンツ鍵・利用条件の配信方式の決定方法のフローチャートである。

図 12 (a) は、パラメータがコンテンツの圧縮フォーマットである場合の配信方式決定ルール DB の管理データの一例を示す図である。

25 図 12 (b) は、パラメータがコンテンツホルダ ID である場合の配信方式決定ルール DB の管理データの一例を示す図である。

図 12 (c) は、パラメータが CBR および VBR の平均レートである場合の配信方式決定ルール DB の管理データの一例を示す図である。

30 図 12 (d) は、パラメータがコンテンツ利用条件である場合の配信方式決定ルール DB の管理データの一例を示す図である。

図 13 は、ユーザ登録のフローチャートである。

図 14 は、コンテンツ利用までのフローチャートである。

図 1 5 は、クライアント機器の構成を示す機能ブロック図である。

図 1 6 は、クライアント機器での再生処理を示すフローチャートである。

図 1 7 は、コンテンツ鍵の配信方式を示す情報が暗号化コンテンツデータに重畳されている場合におけるコンテンツのデータ構造の一例を示す図である。

DESCRIPTION OF THE PREFERRED EMBODIMENT(S)

以下、本発明の実施の形態について、図 1 から図 1 7 を参照して説明する。

図 1 に実施の形態に係る動画コンテンツ配信サービスシステムの概念図を示す。クライアント機器 1 1 0 は、インターネットなどの通信路 1 3 0 を通じて、コンテンツ配信管理サーバ 1 2 1、マルチキャスト配信サーバ 1 2 2、ユニキャスト配信サーバ 1 2 3、暗号化コンテンツ配信サーバ 1 2 4、ユーザ管理サーバ 1 2 0 に接続されている。また、コンテンツ配信管理サーバ 1 2 1 は、インターネットなどの通信路 1 3 0 を通じて、マルチキャスト配信サーバ 1 2 2、ユニキャスト配信サーバ 1 2 3、暗号化コンテンツ配信サーバ 1 2 4、ユーザ管理サーバ 1 2 0 に接続されている。また、マルチキャスト配信サーバ 1 2 2、ユニキャスト配信サーバ 1 2 3 をまとめてコンテンツ鍵配信サーバと呼ぶ。

本システムを用いた動画コンテンツ配信サービスは、予めユーザ登録をしたユーザがクライアント機器 1 1 0 を利用してインターネットなどの通信路 1 3 0 を介して動画コンテンツを再生できる環境を提供するサービスである。

ユーザに配信されるコンテンツは、コンテンツホルダにより暗号化され、一旦、コンテンツ配信管理サーバ 1 2 1 を経由して、マルチキャスト配信サーバ 1 2 2 又は暗号化コンテンツ配信サーバ 1 2 4 に登録される。

ユーザは暗号化コンテンツをマルチキャスト配信サーバ 1 2 2 又は暗号化コンテンツ配信サーバ 1 2 4 から取得する。コンテンツを復号するための鍵（以下、コンテンツ鍵）及びコンテンツ利用条件は、マルチキャスト配信サーバ 1 2 2、ユニキャスト配信サーバ 1 2 3 のいずれかのコンテンツ鍵配信サーバから配信される。コンテンツ鍵がユニキャスト配信されるコンテンツは暗号化コンテンツ配信サーバ 1 2 4 に登録され、コンテンツ鍵がマルチキャスト配信されるコンテンツはマルチキャスト配信サーバ 1 2 2 に登録

される。

コンテンツ利用条件とは、ユーザがコンテンツを利用する際の制限事項であり、再生可能回数、再生可能期間、再生可能時間等が設定される。クライアント機器 110 は、取得した暗号化コンテンツをコンテンツ鍵で復号し、
5 コンテンツ利用条件に従って再生する。再生可能回数とは、コンテンツを利用する回数の制限であり、コンテンツを利用する度にその回数は減少し、0 になると利用できなくなる。再生可能期間とは、コンテンツを利用することのできる期間であり、コンテンツを利用する日時がその期間内であるときのみ利用可能である。再生可能時間とは、コンテンツを利用することができる
10 残り時間であり、コンテンツを利用した時間分、減少し、0 になると利用できなくなる。

本システムの構成要素について説明する。

クライアント機器 110 は、ユーザがコンテンツを再生する機器である。また、クライアント機器 110 は、その機器を一意に識別するための識別子
15 であるクライアント ID を持つ。クライアント ID は工場出荷時に設定され、出荷後はユーザによって変更されることはない。なお、クライアント機器 110 はユニキャスト配信及びマルチキャスト配信による本システムの配信を受けることが可能であることをクライアント ID により確認することができる。

ユーザ管理サーバ 120 は、本システムを用いたコンテンツ配信サービス
20 に加入しているユーザの管理を行う。ユーザ管理サーバ 120 は、ユーザ管理データベース（以下、「DB」と略記する。）180 を備える。ユーザ管理 DB 180 では、ユーザを一意に識別するためのユーザ ID、ユーザ名、ユーザを認証するためのパスワード、ユーザの使用するクライアント機器 110 のクライアント ID などを保持し管理する。
25

ユーザ管理 DB 180 で保持し管理するデータの一例を図 2 に示す。

図 2 では、ユーザ名 “User 1” には、ユーザ ID “User_1111”、パスワード “a a a b b b c c c” が設定され、クライアント ID “123__a b c” のクライアント機器 110 を所有していることを示している。
30 ユーザ ID はユーザ登録の際、ユーザ管理サーバで割り当てられ、パスワードはユーザ自身が設定する。

コンテンツ配信管理サーバ 121 は、コンテンツホルダからのコンテンツ

配信要求を受け、コンテンツ鍵およびコンテンツ利用条件の配信方式を決定する機能を持つ。また、コンテンツホルダの管理、各コンテンツの配信方式の管理を行う。コンテンツ配信管理サーバ121は、コンテンツホルダ管理DB140、コンテンツ配信方式管理DB141、配信方式決定ルールDB142を備える。コンテンツホルダ管理DB140では、コンテンツの配信要求を受け付けるコンテンツホルダに関する情報を保持し管理するため、コンテンツホルダを一意に識別するためのコンテンツホルダID、コンテンツホルダ名、認証のためのパスワードなどを保持する。図3に、コンテンツホルダ管理DB140で保持し管理するデータの一例を示す。

図3では、例えば、コンテンツホルダ名“C__HOLDER__1”には、コンテンツホルダID“Holder__1111”、パスワード“a b c r s t”が設定されていることを示している。

コンテンツ配信方式管理DB141では、コンテンツを一意に識別するためのコンテンツID、コンテンツ名、コンテンツを提供するコンテンツホルダのコンテンツホルダID、コンテンツの圧縮フォーマット、コンテンツ鍵およびコンテンツ利用条件の配信方式、コンテンツの再生時間、暗号化コンテンツのデータサイズなどを保持し管理する。図4に、コンテンツ配信方式管理DB141で保持及び管理するデータの一例を示す。

図4では、例えば、コンテンツ名“世界の山脈”は、コンテンツID“CONT__0001”で表され、コンテンツホルダID“Holder__1111”が所有するコンテンツであり、圧縮フォーマットが“MPEG-2”、配信方式が“ユニキャスト方式”、再生時間“60分”、データサイズが“1,500MB”であることを示している。

配信方式決定ルールDB142では、コンテンツに応じて配信方式を決定するためのルールを保持し管理する。配信方式決定ルールDB142で保持及び管理するデータの詳細については後述する。

マルチキャスト配信サーバ122は、コンテンツ鍵およびコンテンツ利用条件を予め設定された時間にユーザ管理サーバ120で管理されているユーザの所有するクライアント機器110に対してIPマルチキャストにより毎日配信する。マルチキャスト配信サーバ122は、配信スケジュールDB150およびマルチキャストコンテンツDB151を備える。配信スケジュールDB150は、コンテンツ鍵をマルチキャストで配信する時間、配信

するコンテンツ鍵で再生可能なコンテンツのコンテンツID、配信するコンテンツ鍵およびコンテンツ利用条件などを保持し管理する。マルチキャストコンテンツDB151は、コンテンツ鍵がマルチキャスト配信により配信されるコンテンツについてのみ、暗号化コンテンツデータを格納する。図5は、
5 配信スケジュールDB150で保持し管理する配信スケジュール表の一例を示す図である。

図5(a)で示すように、コンテンツID“CONT_0001”のコンテンツはコンテンツ鍵“0xaaaa...aaaa”により暗号化されている。コンテンツID“CONT_0001”のコンテンツ利用条件には“再生回数3回”という制限が設定されており、“12:00”にコンテンツ鍵が配信されるように設定されている。この他に、配信スケジュール表には、マルチキャストコンテンツDB151内の各コンテンツの格納場所を示すファイルパスなどが記述されている。
10

ユニキャスト配信サーバ123は、ユーザ管理サーバ120で管理されているユーザから要求があった場合に、コンテンツ鍵およびコンテンツ利用条件を配信するサーバである。ユニキャスト配信サーバ123は、配信データ管理DB160を備える。配信データ管理DB160では、配信するコンテンツ鍵で再生可能なコンテンツのコンテンツID、配信するコンテンツ鍵およびコンテンツ利用条件を保持し管理する。配信データ管理DB160で管理するデータの一例を図6に示す。図6では、コンテンツID“CONT_0001”のコンテンツはコンテンツ鍵“0x1111...1111”により暗号化されている。コンテンツID“CONT_0001”のコンテンツ利用条件には“再生回数3回”という制限設定されていることを示している。
15
20

暗号化コンテンツ配信サーバ124は、ユーザが暗号化コンテンツをダウンロードするためのサーバである。暗号化コンテンツ配信サーバ124は、暗号化コンテンツ管理DB170およびユニキャストコンテンツDB171を備える。暗号化コンテンツ管理DB170では、コンテンツID、暗号化コンテンツのデータサイズおよび暗号化されたコンテンツデータが格納されているファイルパスなどを保持し管理する。ユニキャストコンテンツDB171は、コンテンツ鍵がユニキャストにより配信されるコンテンツについて、暗号化コンテンツデータを格納する。図7に、暗号化コンテンツ管理DB170で保持及び管理するデータの一例を示す。図7では、コンテンツ
25
30

ID “CONT__0001” の暗号化コンテンツデータのサイズは “1, 500MB” であり、コンテンツ鍵の配信方式はユニキャスト配信であり、暗号化コンテンツデータはユニキャストコンテンツDB171の “C: ¥ content ¥ cont__0001. enc” に格納されていることを示している。

図8（a）および図8（b）に、マルチキャストコンテンツDB151に格納される暗号化コンテンツとユニキャストコンテンツDB171に格納される暗号化コンテンツとのデータ構造の相違を示す。図8（a）は、図1に示したユニキャストコンテンツDB171に格納される暗号化コンテンツのデータ構造を示す図である。図8（b）は、図1に示したマルチキャストコンテンツDB151に格納される暗号化コンテンツのデータ構造を示す図である。図8（a）に示すように、コンテンツ鍵がユニキャストで配信されるコンテンツは、コンテンツIDと暗号化コンテンツデータとから構成されている。これに対し、コンテンツ鍵がマルチキャスト配信されるコンテンツは、図8（b）に示すように、コンテンツID、コンテンツ鍵、コンテンツ利用条件および暗号化コンテンツデータなどから構成されている。すなわち、図8（a）のコンテンツに、さらに、コンテンツ鍵およびコンテンツ利用条件が重畳されている。コンテンツ鍵及びコンテンツ利用条件の部分のデータについては、特定のクライアント機器110のみ利用可能とするため、受信データを利用できるクライアント機器110を限定する機能を用いて保護されているものとする。具体的には、コンテンツに重畳され、マルチキャストされるコンテンツ鍵及びコンテンツ利用条件は、あらかじめ暗号化されているものとする。暗号化されたコンテンツ鍵及びコンテンツ利用条件を復号するための復号鍵は、ユーザ登録したユーザにのみ配布される。この復号鍵の配布方法には、あらかじめ復号鍵がROM（Read Only Memory）などの不揮発性メモリに書き込まれたクライアント機器110をユーザ登録したユーザに配布する方法や、この復号鍵が記録された記録媒体をユーザ登録したユーザに配布する方法などがある。これにより、ユーザ登録をしたユーザのクライアント機器110は、ROMや配布された記録媒体などから復号鍵を読み出して、マルチキャストされたコンテンツに重畳されているコンテンツ鍵及びコンテンツ利用条件を復号することができる。この復号されたコンテンツ鍵を用いて、当該クライアント機器110は、暗号化コンテン

ツを復号し、その後、復号されたコンテンツ利用条件に従ってコンテンツを利用することができる。なお、暗号化されたコンテンツ鍵を復号するための復号鍵は、必ずしもROMや記録媒体に記録されて配布される必要はなく、ユーザ登録をしたユーザに、あらかじめセキュアな通信により配布されてい

5 ればよい。この暗号化方法については、非特許文献：中野他、“デジタルコンテンツ保護用鍵管理方式”、2001年暗号と情報セキュリティシンポジウム講演論文集、5A-5、2001に詳しい。なお、マルチキャストされるコンテンツ鍵及びコンテンツ利用条件を、ユーザ登録したユーザにだけ利用できるようにする方法は、デジタルコンテンツ保護用鍵管理方式に限定され

10 ず、他の方法であってもよい。このようなデータ構造を持つ暗号化コンテンツは、コンテンツ配信管理サーバ121によって生成され、マルチキャストコンテンツDB151に格納されてもよいし、マルチキャスト配信サーバ122によって生成され、マルチキャストコンテンツDB151に格納されてもよい。

15 コンテンツ登録用端末100は、コンテンツホルダがコンテンツ配信管理サーバ121に配信するコンテンツの登録を行う際に用いる端末である。コンテンツの登録については後述する。

以下、サービス内の各処理について、コンテンツホルダによる配信コンテンツの登録、配信方式の決定方法、ユーザによるユーザ登録、ユーザのコン

20 テンツ利用について順に説明する。

まず、コンテンツホルダによる配信コンテンツの登録について説明する。

コンテンツホルダは、コンテンツ配信管理サーバ121に対し、コンテンツ登録用端末100を用いてコンテンツ登録要求を行う。図9にコンテンツホルダによるコンテンツ登録処理のフローチャートを示す。

25 コンテンツ配信管理サーバ121は、コンテンツホルダからの配信コンテンツの登録要求を受ける前に、コンテンツホルダの認証を行う。本実施の形態においては、コンテンツホルダは事前にコンテンツホルダ管理DB140に登録されている必要がある。コンテンツホルダは、配信コンテンツ登録要求時にコンテンツ登録用端末100を用いて、通信路130を介しコンテ

30 ツ配信管理サーバ121へコンテンツホルダIDとパスワードを送信する。コンテンツ配信管理サーバ121は受信したコンテンツホルダIDとパスワードの組をコンテンツホルダ管理DB140に登録されているデータと

照会することでログインの成否を判定する（S901）。

コンテンツホルダはコンテンツ配信管理サーバ121でのログインが成功した後（S902）、コンテンツ配信管理サーバ121に対し、配信するコンテンツの登録要求を送る（S903）。この際、コンテンツホルダは、
5 暗号化コンテンツ、コンテンツ鍵、コンテンツ利用条件、コンテンツメタデータを送信する。本実施の形態では、コンテンツの圧縮フォーマットはMP
EG-2であり、コンテンツは128ビットの鍵を用いてAES（A d v a
n c e d E n c r y p t i o n S t a n d a r d）で暗号化されている。
MPEG-2についてはISO/IEC 13818、AESについてはF
10 IPS-197に詳しい。

メタデータにはコンテンツを一意に識別する「コンテンツID」、「コンテ
ンツ名」、「コンテンツホルダ名」、コンテンツの「圧縮フォーマット」、「再
生時間」、「暗号化コンテンツのデータサイズ」が記述されている。図10に
メタデータの一例を示す。図10では、コンテンツID“CONT_000
15 1”のコンテンツのコンテンツ名は“世界の山脈”であり、このコンテンツ
を提供したコンテンツホルダは“コンテンツホルダ_ABC”である。圧縮
フォーマットは“MP EG-2”であり、再生時間は“60分”、暗号化コ
ンテンツのデータサイズは“1, 500MB”である。なお、メタデータに
は、他に「製作年度」、圧縮率「CBR（Constant Bit Rate）、およびVB
20 R（Variable Bit Rate）の平均レート」等が含まれても構わない。

コンテンツ配信管理サーバ121は、コンテンツホルダからコンテンツ登
録要求で受け取ったメタデータ中のコンテンツ圧縮フォーマットと配信方
式決定ルールDB142とから登録するコンテンツ鍵の配信方式を決定す
る（S904）。コンテンツ鍵の配信方式決定方法については後述する。

ユニキャスト配信と決定された場合（S905）、コンテンツ配信管理サ
ーバ121はコンテンツ鍵、コンテンツ利用条件、メタデータ、及びコンテ
ンツ配信条件をユニキャスト配信サーバ123へ登録する（S906）。併
せて、コンテンツ配信管理サーバ121は、その暗号化コンテンツデータを
暗号化コンテンツ配信サーバ124に登録する。ユニキャスト配信サーバ1
30 23が持つ配信データ管理DB160で保持及び管理するデータは図6に
あるデータを用いる。

マルチキャスト配信と決定された場合（S905）、コンテンツ配信管理

サーバ121はコンテンツ鍵、コンテンツ利用条件、メタデータ及び暗号化コンテンツデータをマルチキャスト配信サーバ122へ登録する（S907）。マルチキャスト配信サーバ122では、新たに登録された暗号化コンテンツデータをマルチキャストコンテンツDB151に格納し、配信スケジュールの空いている時間に新たに登録されたコンテンツの配信スケジュールを追加し、配信スケジュールDB150を更新する。

図5に配信スケジュールDB150の更新の様子を示す。図5（a）に示すように、更新前の配信スケジュールDB150に対し、コンテンツID“CONT__0002”、コンテンツ鍵“0xbbbb・・・bbb（128bit）”、コンテンツ利用条件“再生回数1回”のコンテンツの配信スケジュールを追加する場合を考える。更新前には“13：00”の配信スケジュールが空いているため、その時間を、追加するコンテンツの配信スケジュールとして設定し、配信スケジュールDB150を更新すると、図5（b）に示す更新後の配信スケジュールDBの状態になる。

コンテンツ配信管理サーバ121は、決定した配信方式に従って各配信サーバにコンテンツ鍵、コンテンツ利用条件を登録後、コンテンツ鍵がユニキャスト配信される暗号化コンテンツを暗号化コンテンツ配信サーバ124へ登録し（S908）、処理を終了する。

次に、図9に示したS904のコンテンツ鍵の配信方式の決定方法の処理の詳細について図11を用いて説明する。

コンテンツ配信管理サーバ121はコンテンツホルダからコンテンツメタデータを受信した後、コンテンツ鍵及びコンテンツ利用条件の配信方式を決定する。具体的には、まず、コンテンツ配信管理サーバ121はコンテンツ鍵配信方式決定ルールを、配信方式決定ルールDB142より取得する（S1001）。

本実施の形態では、コンテンツの圧縮フォーマットによって、コンテンツを利用するユーザ数が変わることを想定し、コンテンツのメタデータ中に記述されるコンテンツ圧縮フォーマットを、コンテンツ鍵及びコンテンツ利用条件の配信方式決定のためのパラメータとする。

図12（a）に、本実施の形態の配信方式決定ルールDB142で保持し管理するデータ（配信方式決定ルール）の一例を示す。このルールでは、登録するコンテンツのメタデータ中にある圧縮フォーマットを配信方式決定

のパラメータとしている。そのパラメータを用いて、配信方式決定ルールに従って配信方式を決定する（S 1 0 0 2）。この場合、圧縮フォーマットが M P E G - 2、又は A V I（Audio、Video、 still Images）の場合にはユニキャスト配信、M P E G - 4 の場合にはマルチキャスト配信を選択するように設定されている。M P E G - 4 については I S O / I E C 1 4 4 9 6 に詳しい。

以下、上記配信方式決定ルール D B 1 4 2 で管理されるデータ（配信方式決定ルール）の他の例について説明する。

図 1 2（b）に、コンテンツホルダに応じて配信方式を変更するような要求があることを想定し、コンテンツ配信方式を決定するパラメータをコンテンツホルダ I D にした場合の配信方式決定ルールの一例を示す。コンテンツホルダ I D “H o l d e r _ 1 1 1 1” および “H o l d e r _ 3 3 3 3” の場合にはユニキャスト配信、コンテンツホルダ I D “H o l d e r _ 2 2 2 2” の場合にはマルチキャスト配信を選択するように設定されている。

図 1 2（c）に、コンテンツの画質によりコンテンツを利用するユーザ数が変わることを想定し、コンテンツ配信方式を決定するパラメータを C B R および V B R の平均レートにした場合の配信方式決定ルールの一例を示す。ここでは、C B R および V B R の平均レートが 5 0 0 k b p s 未満の場合にはマルチキャスト配信、5 0 0 k b p s 以上 1 5 M b p s 未満の場合、および 1 5 M b p s 以上の場合にはユニキャスト配信をそれぞれ選択するように設定されている。

図 1 2（d）に、コンテンツが最初に配信されてからの経過時間により配信方式を変更する要求があることを想定し、コンテンツ配信方式を決定するパラメータをコンテンツ利用条件にした場合の配信方式決定ルールの一例を示す。コンテンツ利用条件が、“再生回数 3 回” の場合および“再生期間 2 0 0 3 / 0 1 / 0 1 ~ 2 0 0 3 / 0 1 / 3 1” の場合にはユニキャスト配信、“再生回数 制限無し” および“再生期間 2 0 0 3 / 0 2 / 0 1 ~ 2 0 0 3 / 0 2 / 2 8” の場合にはマルチキャスト配信をそれぞれ選択するように設定されている。

次にユーザ登録の動作について図 1 3 を用いて説明する。

ユーザはコンテンツを利用する際、ユーザ管理サーバ 1 2 0 に事前にユーザ登録しておく。より具体的には、まず、ユーザはクライアント機器 1 1 0

を用いて、ユーザ管理サーバ120に対し、登録要求を行う。次いで、ユーザ名、パスワード、及びユーザが利用するクライアント機器110のクライアントIDをユーザ管理サーバへ送信する(S1201)。ただし、クライアント機器110のクライアントIDは、ユーザがユーザ名およびパスワードとともに手入力してもよいが、ユーザが入力したユーザ名およびパスワードにクライアント機器110がクライアントIDを自動的に添付して送信するのが一般的である。ユーザの登録要求を受けたユーザ管理サーバ120では、ユーザIDを割り当て(S1202)、ユーザ管理DB180へのデータ追加(S1203)を行い、ユーザ登録終了をクライアント機器110へ通知して終了する。

次にユーザのコンテンツ利用の動作について図14を用いて説明する。

コンテンツ利用のサービスは、ユーザ登録したユーザにのみ提供されるものであり、一旦ユーザ管理サーバ120で認証をする必要がある。そのため、認証に必要なデータの送受信がクライアント機器110とユーザ管理サーバ120との間で行われる(S1301)。クライアント機器110は認証の成否を判定し、認証が成功した場合のみ、以降の処理を行うことができる(S1302)。

ユーザは、コンテンツを利用する際、コンテンツ配信管理サーバ121から、現在配信を行っているコンテンツに関する情報を取得する(S1303)。

コンテンツに関する情報には、図4のように、コンテンツID、コンテンツ名、コンテンツを提供するコンテンツホルダ名(又はコンテンツホルダID)、圧縮フォーマット、コンテンツ鍵の配信方式、コンテンツの再生時間、暗号化コンテンツのデータサイズなどが含まれている。クライアント機器110は、コンテンツ配信管理サーバ121から取得したコンテンツに関する情報に基づいて、コンテンツの配信を要求するためのコンテンツリストを生成し、ユーザに表示する。

ユーザはコンテンツリストから利用したいコンテンツを選択する(S1304)。クライアント機器110は、コンテンツリストから選択されたコンテンツの配信要求を暗号化コンテンツ配信サーバ124に送信する。暗号化コンテンツ配信サーバ124は、配信要求されたコンテンツのコンテンツ鍵がユニキャスト配信される場合にのみ、暗号化されたコンテンツを配信する。クライアント機器110は、暗号化コンテンツ配信サーバ124から暗号化

コンテンツを取得できた場合、コンテンツ鍵の配信方式がユニキャスト配信であると判定する（S 1 3 0 5）。一方、暗号化コンテンツ配信サーバ 1 2 4 から暗号化コンテンツを取得できなかった場合、クライアント機器 1 1 0 は、コンテンツ鍵の配信方式がマルチキャスト配信であると判定する。

- 5 以下、選択されたコンテンツのコンテンツ鍵、及びコンテンツ利用条件の配信方式別に説明する。

選択したコンテンツのコンテンツ鍵、及びコンテンツ利用条件がユニキャスト配信の場合について説明する。選択されたコンテンツのコンテンツ鍵がユニキャスト配信で配信されていると判定した場合、クライアント機器 1 1 0 は、さらに、選択されたコンテンツのコンテンツ鍵をクライアント機器 1 1 0 の内部に保持しているか否かを調べる（S 1 3 0 6）。選択されたコンテンツのコンテンツ鍵をクライアント機器 1 1 0 がすでに保持している場合は、保持しているコンテンツ鍵を用いてクライアント機器 1 1 0 での再生処理を行う（S 1 3 1 1）。選択されたコンテンツのコンテンツ鍵をクライアント機器 1 1 0 が保持していない場合、ユーザのクライアント機器 1 1 0 とユニキャスト配信サーバ 1 2 4 との間で認証を行い、秘匿性・耐改竄性が保証された通信を行う（S 1 3 0 7）。このような通信方式について本実施の形態では特に手法を記述しないが、SSL（Secure Socket
s L a y e r）等を用いる。SSLについては、A. F r i e r 他、“T
h e S S L 3 . 0 P r o t o c o l”、N e t s c a p e C o m m
u n i c a t i o n s C o r p . N o v . 1 8 , 1 9 9 6 に詳しい。なお、
クライアント機器 1 1 0 とユニキャスト配信サーバ 1 2 3 との間で認証は
P K I 方式や共通鍵方式による認証でも構わない。前述の通信によって、ク
ライアント機器 1 1 0 はコンテンツ鍵及びコンテンツ利用条件をユニキャ
スト配信サーバ 1 2 3 から取得する（S 1 3 0 8）。ステップ S 1 3 0 7 に
おいて、ユニキャスト配信サーバ 1 2 3 との認証に失敗した場合、クライ
アント機器 1 1 0 は処理を終了する。

選択されたコンテンツのコンテンツ鍵、及びコンテンツ利用条件がマルチキャスト配信の場合について説明する。選択されたコンテンツのコンテンツ
鍵がマルチキャスト配信で配信されていると判定した場合、クライアント機
器 1 1 0 は、選択されたコンテンツのコンテンツ鍵をクライアント機器 1 1
0 の内部に保持しているか否かを調べる（S 1 3 0 9）。選択されたコンテ

コンテンツ鍵をクライアント機器 110 がすでに保持している場合は、保持しているコンテンツ鍵を用いてクライアント機器 110 での再生処理を行う（S 1311）。選択されたコンテンツのコンテンツ鍵をクライアント機器 110 が保持していない場合、クライアント機器 110 は、マルチキャスト配信サーバ 122 からコンテンツ鍵の配信を受ける。マルチキャスト配信の場合、マルチキャスト配信サーバ 122 は予め設定された配信スケジュールに基づき、コンテンツ、コンテンツ鍵及びコンテンツ利用条件をマルチキャストする。クライアント機器 110 はコンテンツ鍵及びコンテンツ利用条件がクライアント機器 110 内に保持されていないため、次のマルチキャストによる配信まで待機する（S 1310）。マルチキャスト配信のスケジュールについては、クライアント機器 110 はマルチキャスト配信サーバ 122 から取得することが可能である。本実施の形態でのマルチキャストによる配信方式は、ユーザ管理サーバ 120 で管理されているユーザの利用するクライアント機器 110 にのみ配信する必要があるため、受信データを利用できるクライアント機器 110 を限定する機能を備えた配信方式で実現する。具体的実現方法については、非特許文献：中野他、“デジタルコンテンツ保護用鍵管理方式、” 2001 年暗号と情報セキュリティシンポジウム講演論文集、5A-5、2001 に詳しい。

各配信処理ともに、コンテンツ、コンテンツ鍵、及びコンテンツ利用条件を取得した後、クライアント機器 110 内部での再生処理が行われる（S 1311）。

次に、図 14 のステップ S 1311 におけるクライアント機器 110 内部での再生処理の詳細について、図 15、及び図 16 を用いて説明する。図 15 は、クライアント機器 110 の構成を示す機能ブロック図である。図 16 は、図 14 のステップ S 1311 におけるクライアント機器 110 内部でのコンテンツ再生処理の動作を示すフローチャートである。

クライアント機器 110 は、通信部 1401、利用条件判定部 1402、暗号化コンテンツ蓄積部 1403、コンテンツ復号部 1404、コンテンツデコード部 1405、クライアント ID 蓄積部 1406、コンテンツ鍵蓄積部 1407、入力部 1408、要求処理部 1409、配信方式判定部 1410 および画面出力部 1411 を備える。

通信部 1401 は、各種サーバと通信するための機能処理部である。利用

条件判定部 1 4 0 2 は、コンテンツの新たな利用がコンテンツ利用条件を満たしているかを判定する機能処理部である。暗号化コンテンツ蓄積部 1 4 0 3 は、暗号化コンテンツを蓄積する記憶部および機能処理部である。図 1 4 のステップ S 1 3 0 5 またはステップ S 1 3 0 8 で取得された暗号化コンテンツは、暗号化コンテンツ蓄積部 1 4 0 3 に蓄積される。コンテンツ復号部 1 4 0 4 は、コンテンツ鍵を用いて暗号化コンテンツの復号を行う機能処理部である。

コンテンツデコード部 1 4 0 5 は、コンテンツの圧縮フォーマットに応じてコンテンツをデコードし、映像および音声データを出力する機能処理部である。クライアント ID 蓄積部 1 4 0 6 は、クライアント ID を蓄積する記憶部および機能処理部であり、サーバとの通信においてクライアント ID の送信が必要なとき、通信部 1 4 0 1 はここからクライアント ID を取得する。コンテンツ鍵蓄積部 1 4 0 7 は、コンテンツ鍵及びコンテンツ利用条件を蓄積する記憶部および機能処理部である。図 1 4 のステップ S 1 3 0 8 で取得されたコンテンツ鍵およびコンテンツ利用条件は、コンテンツ鍵蓄積部 1 4 0 7 に蓄積される。入力部 1 4 0 8 はユーザからの要求を入力する機能処理部である。要求処理部 1 4 0 9 は、入力部 1 4 0 8 より入力された要求に応じて処理を行う機能処理部である。配信方式判定部 1 4 1 0 は、ユーザによって選択されたコンテンツのコンテンツ鍵が、マルチキャストで配信されるか、ユニキャストで配信されるかのいずれであるかを判定する。画面出力部 1 4 1 1 は再生する動画やサーバからの情報を描画し、ユーザに提示する機能処理部である。

クライアント機器 1 1 0 は、コンテンツ鍵蓄積部 1 4 0 7 に格納されているコンテンツ鍵、およびコンテンツ利用条件を取得した後、利用条件判定部 1 4 0 2 にて、現在時刻におけるコンテンツの新たな利用が、取得されたコンテンツ利用条件に示される条件を満たしているか確認をする（S 1 5 0 1）。例えば、再生可能回数が 0 でないかの確認や、コンテンツを再生する日時が再生可能期間内であるかの確認である。コンテンツ利用条件が満足されている場合、利用条件判定部 1 4 0 2 はコンテンツ鍵蓄積部 1 4 0 7 に格納されているコンテンツ鍵をコンテンツ復号部 1 4 0 4 へ送信する（S 1 5 0 1）。コンテンツ復号部 1 4 0 4 は、暗号化コンテンツ蓄積部 1 4 0 3 より当該暗号化コンテンツを取得し、利用条件判定部 1 4 0 2 より取得したコ

ンテンツ鍵を用いて復号する（S 1 5 0 2）。復号化されたデータをコンテンツデコード部 1 4 0 5 へ送信する。コンテンツデコード部 1 4 0 5 は、圧縮フォーマットに応じてコンテンツをデコードし、映像および音声データを出力し（S 1 5 0 3）、処理を終了する。

5 以上のように、本実施の形態のコンテンツ配信システム 2 0 0 によれば、コンテンツ及びコンテンツ鍵などを配信する側では、各コンテンツの属性に応じて、コンテンツ鍵及びコンテンツ利用条件の配信方式を切り替えて配信することができる。これにより、例えば、同一のコンテンツに対し、コンテンツ鍵及びコンテンツ利用条件の配信要求が殺到することが予測される場合
10 合には、そのコンテンツ鍵及びコンテンツ利用条件をマルチキャストによって配信し、コンテンツ配信システム 2 0 0 内のサーバ負荷を低減することができる。また、コンテンツの著作権保護の方が、コンテンツ配信システム 2 0 0 のサーバ負荷よりも優先される場合には、コンテンツ鍵及びコンテンツ利用条件をユニキャストによって配信し、著作権の安全性を向上することができる。
15 また、クライアント機器 1 1 0 側では、内部の配信方式判定部 1 4 1 0 でコンテンツ鍵及びコンテンツ利用条件の配信方式を判定することができるので、コンテンツ毎に異なる配信方式で配信されるコンテンツ鍵及びコンテンツ利用条件を、支障なく取得することができる。これによって、何ら問題なく所望のコンテンツを利用することができる。

20 なお、コンテンツ配信管理サーバ 1 2 1、マルチキャスト配信サーバ 1 2 2、ユニキャスト配信サーバ 1 2 3、暗号化コンテンツ配信サーバ 1 2 4、ユーザ管理サーバ 1 2 0 は独立でなく、一つのサーバが別のサーバの機能を兼ねてもよい。

 なお、マルチキャストによる配信は毎日行われなくてもよい。

25 なお、コンテンツ鍵の配信方式を決定するパラメータは、コンテンツの圧縮フォーマット以外に、コンテンツホルダ ID、CBR および VBR の平均レート、コンテンツ利用条件などでも構わない。

 また、コンテンツ鍵の配信方式を決定するパラメータをいずれにするかは、コンテンツホルダがコンテンツを登録する際に、コンテンツ配信管理サーバ
30 1 2 1 に指定してもよいし、コンテンツ配信管理サーバ 1 2 1 がコンテンツ配信システム 2 0 0 における各サーバの負荷に応じて動的に決定するとしてもよい。

なお、暗号化コンテンツの取得方法としては、メディアによる配信、放送などのブロードキャストによる配信でも構わない。

5 なお、上記実施の形態では、クライアント機器 110 は、所望のコンテンツの配信を暗号化コンテンツ配信サーバ 124 に要求することによって、コンテンツ鍵の配信方式を判定した。すなわち、マルチキャストで配信される
10 コンテンツ鍵およびコンテンツ利用条件はコンテンツに重畳されており、マルチキャスト配信サーバ 122 のみから配信されたが、本発明はこれに限定されない。例えば、クライアント機器 110 は、コンテンツに重畳されている情報を読み取ることによって、コンテンツ鍵の配信方式を判定するとしてもよい。すなわち、コンテンツには、コンテンツ鍵およびコンテンツ利用条件の実体の代わりに、コンテンツ鍵およびコンテンツ利用条件の配信方式を示す情報が重畳されているとしてもよい。図 17 は、コンテンツ鍵の配信方式を示す情報が暗号化コンテンツデータに重畳されている場合における
15 コンテンツのデータ構造の一例を示す図である。同図のように、暗号化コンテンツデータには、コンテンツ ID およびコンテンツ鍵及びコンテンツ利用条件の配信方式を示す情報が重畳される。

20 この場合、コンテンツ配信管理サーバ 121 は、各コンテンツのコンテンツ鍵およびコンテンツ利用条件の配信方式を決定した後、決定された配信方式を示す情報を各コンテンツに重畳し、暗号化コンテンツ配信サーバ 124 に登録する。従って、コンテンツは、コンテンツ鍵およびコンテンツ利用条件の配信方式にかかわらず、暗号化コンテンツ配信サーバ 124 から一元的に配信される。また、コンテンツ配信管理サーバ 121 は、各コンテンツの
25 コンテンツ鍵およびコンテンツ利用条件の配信方式を決定した後、コンテンツ鍵およびコンテンツ利用条件を、決定された配信方式に従って、ユニキャスト配信サーバ 123 およびマルチキャスト配信サーバ 122 に登録する。

30 これに対応して、クライアント機器 110 では、ユーザがコンテンツを利用しようとする際に、まず、暗号化コンテンツ配信サーバ 124 から暗号化コンテンツを取得する。その後、配信方式判定部 1410 は、取得された暗号化コンテンツに重畳されている情報から、コンテンツ鍵及びコンテンツ利用条件の配信方式を判定し、判定結果に従って、対応するサーバからコンテンツ鍵及びコンテンツ利用条件を取得する。すなわち、コンテンツ鍵及びコンテンツ利用条件の配信方式がマルチキャストであると判定した場合には、

マルチキャスト配信サーバ 1 2 2 からコンテンツ鍵及びコンテンツ利用条件が配信されるのを待機し、コンテンツ鍵及びコンテンツ利用条件の配信方式がユニキャストであると判定した場合には、ユニキャスト配信サーバ 1 2 3 にコンテンツ鍵及びコンテンツ利用条件の配信を要求する。以下、クライアント機器 1 1 0 におけるコンテンツの再生処理は、図 1 6 を用いてすでに説明したとおりである。

さらに、クライアント機器 1 1 0 は、コンテンツ鍵およびコンテンツ利用条件の配信方式を特定するための情報を、サーバから取得するとしてもよい。具体的には、クライアント機器 1 1 0 は、図 1 4 に示したステップ S 1 3 0 3 の処理において、コンテンツ配信管理サーバ 1 2 1 に対し、コンテンツに関する情報を要求する。コンテンツ配信管理サーバ 1 2 1 はクライアント機器 1 1 0 の要求に応じ、コンテンツ配信方式管理 DB 1 4 1 から図 4 に示したデータ（コンテンツに関する情報）を読み出して、クライアント機器 1 1 0 に送信する。クライアント機器 1 1 0 は、コンテンツ配信管理サーバ 1 2 1 から取得したコンテンツに関する情報を参照して、コンテンツ鍵の配信方式を判定し、判定された配信方式に応じたサーバからコンテンツ鍵及びコンテンツ利用条件を取得する。

この方法によれば、クライアント機器 1 1 0 は、コンテンツをコンテンツ鍵およびコンテンツ利用条件よりも先に取得しておく必要はなく、コンテンツ鍵およびコンテンツ利用条件を取得した後にコンテンツを取得しても、問題なくコンテンツを利用することができる。

なお、暗号化コンテンツは、コンテンツ鍵の配信方式にかかわらず、すべて図 8 (a) に示したデータ構造とし、暗号化コンテンツ配信サーバ 1 2 4 が一元的に管理し配信するとしてもよい。もちろん、上記実施の形態と同様に、コンテンツ鍵がユニキャストで配信されるコンテンツのみ図 8 (a) に示したデータ構造で、暗号化コンテンツ配信サーバ 1 2 4 から配信され、コンテンツ鍵がマルチキャストで配信されるコンテンツは図 8 (b) に示したデータ構造で、マルチキャスト配信サーバ 1 2 2 から配信されるとしてもよい。また、ユニキャスト配信サーバ 1 2 3 の負荷が大きくなるが、暗号化コンテンツ配信サーバ 1 2 4 をなくして、その代わりにユニキャスト配信サーバ 1 2 3 もマルチキャスト配信サーバ 1 2 2 も、図 8 (b) に示したデータ構造のコンテンツを配信するとしてもよい。

なお、コンテンツ配信管理サーバ１２１は、クライアント機器１１０の要求に対して、図４に示したようにリストになったコンテンツに関する情報をそのまま送信するのではなくてもよい。例えば、クライアント機器１１０は、利用しようとするコンテンツ毎に、コンテンツ鍵およびコンテンツ利用条件の配信方式を問い合わせるとしてもよい。これに対し、コンテンツ配信管理サーバ１２１は、問い合わせのあったコンテンツについてのみ、コンテンツ鍵及びコンテンツ利用条件の配信方式を回答するとしてもよい。このようにすれば、コンテンツ配信管理サーバ１２１の処理負荷が大きくなるが、クライアント機器１１０において配信方式を判定するための処理負荷が小さくなる。

さらに、コンテンツ配信管理サーバ１２１がクライアント機器１１０の要求に応答してコンテンツに関する情報を送信する代わりに、コンテンツに関する情報を放送やマルチキャストなどにより、あらかじめクライアント機器１１０に配布しておくとしてもよい。

本発明のクライアント機器は、通信機能を備えるコンテンツ再生装置、パーソナルコンピュータ、ＰＤＡ（Personal Digital Assistant）、携帯電話機、ＳＴＢ（Set Top Box）などとして有用である。